

Kevin Fu

Department of Computer Science
University of Massachusetts Amherst
kevinfu@cs.umass.edu
<http://www.cs.umass.edu/~kevinfu/>

Computer Science Building
140 Governors Drive
University of Massachusetts
Amherst, MA 01003-9264

Research areas Trustworthy computing and low-power embedded systems, including systems security and privacy, medical devices, RFID-scale computation, and energy-aware architectures.

Education **Massachusetts Institute of Technology** Cambridge, MA
PhD in Electrical Engineering and Computer Science, 2005.
Thesis: Integrity and access control in untrusted content distribution networks
Advisors: Frans Kaashoek and Ron Rivest

Massachusetts Institute of Technology Cambridge, MA
MEng in Electrical Engineering and Computer Science, 1999.
Thesis: Group sharing and random access in cryptographic storage file systems
Advisor: Ron Rivest

Massachusetts Institute of Technology Cambridge, MA
SB in Computer Science and Engineering, 1998.

Academic positions **Department of Computer Science, UMass Amherst** Amherst, MA
Associate professor w/ tenure, 2011–.
Assistant professor, 2005–2011.
Research scientist, *Summer 2005*.

Awards, honors **ACM SIGCOMM Best Paper Award**
“They Can Hear Your Heartbeats: Non-Invasive Security for Implanted Medical Devices”
at ACM SIGCOMM. 223 submissions. 14% acceptance. *August 2011*.

**UMass Commercial Ventures & Intellectual Property
Technology Development Fund Award**
Award for low-power “SMASH Memory.” *March 2011*.

Association of Computing Machinery (ACM) Senior Member
The Senior Member Grade recognizes those ACM members with at least 10 years of professional experience and 5 years of continuous Professional Membership who have demonstrated performance that sets them apart from their peers. *February 2011*.

Armstrong Fund for Science, UMass Amherst
John and Elizabeth Armstrong established the Armstrong Fund for Science to recognize researchers with aggressive research visions. *May 2010*.
<http://www.umass.edu/research/armstrongawardees.html>

Alfred P. Sloan Research Fellowship
2009. <http://www.sloan.org/fellowships/page/19>

MIT Technology Review TR35

Innovator of the Year. TR35 list recognizes 35 outstanding innovators under the age of 35 each year. The awards span a wide range of fields, including medicine, computing, communications, electronics, and nanotechnology. *September 2009.*

<http://www.technologyreview.com/TR35/index.aspx?year=2009>

NSF CAREER Award

The Faculty Early Career Development (CAREER) Program. *2009.*

IEEE Security & Privacy (Oakland) Outstanding Paper Award

“Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses” at the IEEE Symposium on Security & Privacy. 249 submissions. 11.2% acceptance. *May 2008.*

UMass Commercial Ventures & Intellectual Property Technology Development Fund Award

Award for “Zero-Power Telemetry for Implantable Medical Devices.” *March 2008.*

Intel Foundation PhD Fellowship Award

Intel Fellows recommend the candidates for this award, which provides a year of support and an opportunity to conduct research at Intel. *June 2004.*

10th USENIX Security Symposium Best Student Paper Award

“Dos and Don’ts of Client Authentication on the Web.” *August 2001.*

ACM International Student Research Contest, First Place Graduate Award

Award for a poster and presentation on the SFS Read-Only File System. *February 2001.*

AT&T Student Research Day

Third place graduate award for a poster on the SFS Read-Only File System. *October 2000.*

USENIX Scholar

The USENIX Scholars Fellowship provides a year of funding to students with exceptional research ability and promise. *January 2000.*

Research experience

U.S. Food and Drug Administration (FDA) Silver Spring, MD
Visiting scientist and consultant. Center for Devices and Radiological Health. *2011–.*

MIT Computer Science and AI Lab Cambridge, MA
Visiting scientist. *2011–2012.*

Beth Israel Deaconess Medical Center, Harvard Medical School Boston, MA
Visiting scientist. Cardiovascular Division. *2009–.*

Microsoft Research Redmond, WA
Visiting researcher. Extreme Computing Group. *July 2009, July 2010.*

Johns Hopkins Information Security Institute Baltimore, MD
Visiting scholar for secure file systems, proxy re-encryption, and RFID security & privacy. *2003–2005.*

MIT Parallel and Distributed Operating Systems Group Cambridge, MA
Research assistant in secure file systems and Web authentication at the MIT Lab for Computer Science. *1998–2005*.

Hewlett-Packard Labs Palo Alto, CA
Internship in cryptographic key regression for secure storage. *Summer 2002*.

MIT Applied Security Reading Group Cambridge, MA
Founded the Applied Security Reading Group at the MIT Lab for Computer Science. Conducted 50 seminars for students, faculty, staff, and guests from industry. The seminar included several invited talks from leading experts in security. *1999–2003*.

Bellcore (Telcordia) — Security Research Group Morristown, NJ
Internship in home automation, secure email revocation, a fast stream cipher for video, and approximate message authentication codes for watermarking images. *Summers 1996–1998 and Fall 1998*.

MIT Media Lab, Gesture and Narrative Language Cambridge, MA
Undergraduate researcher on Renga, a system for children around the world to collaboratively write a story in real time. Fall 1995.

**Industrial
experience**

Sightpath/Cisco Systems Waltham/Boxborough, MA
Software engineer for security issues. *1999–2002*.

MIT Information Systems – Network Security Team Cambridge, MA
Technical support. Responded to intrusions, tracked down computer crackers, reverse engineered encrypted exploits, encouraged the use of secure communication, and assisted law enforcement. *1994–2002*.

Holland Community Hospital Holland, MI
Technical support. Rollout of a paperless medical record system. *1993–1996*.

**Refereed
journal
publications**

[J1] “Half-Wits: Software Techniques for Low-Voltage Probabilistic Storage on Microcontrollers with NOR Flash Memory” by Mastrooreh Salajegheh, Yue Wang, Anxiao (Andrew) Jiang, Erik Learned-Miller, Kevin Fu. To appear in *ACM Transactions on Embedded Computing Systems, Special Issue on Probabilistic Embedded Computing*, 2012.

[J2] “Clinically Significant Magnetic Interference of Implanted Cardiac Devices by Portable Headphones” by Sinjin Lee, Kevin Fu, Tadayoshi Kohno, Benjamin Ransford, and William H. Maisel. In *Heart Rhythm Journal*, 6(10), pp. 1432–1436. October 2009.

[J3] “Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers” by Daniel Holcomb, Wayne Bursleson, and Kevin Fu. In *IEEE Transactions on Computers*, 58(9):1198–1210, September 2009 (earlier version in RFIDSec 2007).

[J4] “Electromagnetic Interference (EMI) of Implanted Cardiac Devices by MP3 Player Headphones” by Sinjin Lee, Benjamin Ransford, Kevin Fu, Tadayoshi Kohno, William H

Maisel. In *Circulation*, 118(18 Supplement), 1 page, November 2008. Abstract 662, 2008 American Heart Association Annual Scientific Sessions.

[J5] “Security and Privacy for Implantable Medical Devices” by Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. In *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, 7(1):30–39, January–March, 2008.

[J6] “Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage” by Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. In *ACM Transactions on Information and System Security (TISSEC)*, 9(1):1–30, February 2006 (earlier version in NDSS 2005).

[J7] “Fast and Secure Distributed Read-Only File System” by Kevin Fu, M. Frans Kaashoek, and David Mazières. In *ACM Transactions on Computer Systems*, 20(1):1–24, February 2002 (fast tracked by OSDI program committee, earlier version in OSDI 2000).

**Refereed
conference
publications**

[C1] “Designing Privacy-preserving Smart Meters with Low-Cost Microcontrollers” by Andres Molina-Markham, George Danezis, Kevin Fu, Prashant Shenoy, David Irwin. To appear in *Proceedings of the 16th International Conference on Financial Cryptography and Data Security*, February 2012.

[C2] “They Can Hear Your Heartbeats: Non-Invasive Security for Implanted Medical Devices” by Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, Kevin Fu. In *Proceedings of ACM SIGCOMM*, 12 pages, August 2011 (**best paper award**, acceptance=32/223=14%).

[C3] “Mementos: System Support for Long-Running Computation on RFID-Scale Devices” by Benjamin Ransford, Jacob Sorber, Kevin Fu. In *Proceedings of 16th Architectural Support for Programming Languages and Operating Systems (ASPLOS 2011)*, 12 pages, March 2011 (acceptance=32/152=21%).

[C4] “Exploiting Half-Wits: Smarter Storage for Low-Power Devices” by Mastrooreh Salajegheh, Yue Wang, Kevin Fu, Anxiao (Andrew) Jiang, Erik Learned-Miller. In *Proceedings of the 9th USENIX Conference on File and Storage Technologies (FAST '11)*, 14 pages, February 2011 (acceptance=20/74=27%).

[C5] “On the Limits of Effective Micro-Energy Harvesting on Mobile CRFID Sensors” by Jeremy Gummesson, Shane S. Clark, Kevin Fu, Deepak Ganesan. In *Proceedings of 8th Annual ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys 2010)*, pp. 195–208, June 2010 (acceptance=25/124=20%).

[C6] “CCCP: Secure Remote Storage for Computational RFIDs” by Mastrooreh Salajegheh, Shane Clark, Benjamin Ransford, Kevin Fu, Ari Juels. In *Proceedings of the 18th USENIX Security Symposium*, pp. 215–230, August 2009 (acceptance=26/176=15%).

[C7] “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses” by Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Rans-

ford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel. In *Proceedings of the 29th IEEE Symposium on Security and Privacy*, pp. 129–142, May 2008 (**outstanding paper award**, acceptance=28/249=11.2%).

[C8] “Maximalist Cryptography and Computation on the WISP UHF RFID Tag” by Hee-Jin Chae, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu. In *Proceedings of the Conference on RFID Security*, 12 pages, July 2007 (acceptance=13/26=50%).

[C9] “Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags” by Daniel E. Holcomb, Wayne P. Bursleson, and Kevin Fu. In *Proceedings of the Conference on RFID Security*, 12 pages, July 2007 (acceptance=13/26=50%).

[C10] “Vulnerabilities in First-Generation RFID-Enabled Credit Cards” by Thomas S. Heydt-Benjamin, Daniel V. Bailey, and Kevin Fu, Ari Juels, Tom O’Hare. In the *Proceedings of 11th International Conference on Financial Cryptography and Data Security*, Lecture Notes in Computer Science, Vol. 4886, pp. 2–14, February 2007 (acceptance=17/84=20%, extended version UMass Amherst Tech Report 06-055, October 2006).

[C11] “Key Regression: Enabling Efficient Key Distribution for Secure Distributed Storage” by Kevin Fu, Seny Kamara, and Tadayoshi Kohno. In *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS)*, 20 pages, February 2006 (acceptance=13.6%).

[C12] “Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage” by Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS)*, 15 pages, February 2005 (acceptance=16/124=12.9%, extended version in ACM TISSEC).

[C13] “REX: Secure, Extensible Remote Execution” by Michael Kaminsky, Eric Peterson, Daniel B. Giffin, Kevin Fu, David Mazières, and M. Frans Kaashoek. In *Proceedings of the 2004 USENIX Annual Technical Conference (USENIX)*, pp. 199–212, June 2004 (acceptance=21/164=13%).

[C14] “Plutus: Scalable Secure File Sharing on Untrusted Storage” by Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian Wang, and Kevin Fu. In *Proceedings of the 2nd USENIX Conference on File and Storage Technologies (FAST)*, pp. 29–42, March 2003 (acceptance=18/67=27%).

[C15] “Dos and Don’ts of Client Authentication on the Web” by Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. In *Proceedings of the 10th USENIX Security Symposium*, pp. 251–268, August 2001 (**best student paper award**, acceptance=28.9%, extended version MIT-LCS Tech Report #818).

[C16] “Fast and Secure Distributed Read-Only File System” by Kevin Fu, M. Frans Kaashoek, David Mazières. In the *Proceedings of the 4th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2000)*, October 2000 (acceptance=24/111=21.6%).

[C17] “Revocation of Unread Email in an Untrusted Network” by Avi Rubin, Dan Boneh, and Kevin Fu. In *Proceedings of the Australasian Conference on Information Security and Privacy*, Springer-Verlag, Lecture Notes in Computer Science, Vol. 1270, pp. 62–75. July 1997.

**Refereed
workshop
publications**

[W1] “Ekho: Bridging the Gap Between Simulation and Reality in Tiny Energy-Harvesting Sensors” by Hong Zhang, Mastooreh Salajegheh, Kevin Fu, Jacob Sorber. In *Workshop on Power Aware Computing and Systems (HotPower 2011)*, 5 pages, October 2011.

[W2] “Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices” by Steve Hanna, Rolf Rolles, Andres Molina-Markham, Pongsin Poosankam, Kevin Fu, Dawn Song. In *Proceedings of 2nd USENIX Workshop on Health Security and Privacy (HealthSec)*, 5 pages, August 2011 (acceptance=13/38=34%).

[W3] “Private Memoirs of a Smart Meter” by Andres Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, David Irwin. In *2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys)*, Zurich, Switzerland, 6 pages, November 2010, in conjunction with ACM SenSys 2010 (acceptance=14/40=35%).

[W4] “HICCUPS: Health Information Collaborative Collection Using Privacy and Security” by Andres Molina, Mastooreh Salajegheh, Kevin Fu. In *ACM Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pp. 21–30, November 2009.

[W5] “Towards Autonomously-Powered CRFIDs” by Shane S. Clark, Jeremy Gummeson, Kevin Fu, Deepak Ganesan. In *Workshop on Power Aware Computing and Systems (HotPower 2009)*, 5 pages, October 2009.

[W6] “Getting Things Done on Computational RFIDs with Energy-Aware Checkpointing and Voltage-Aware Scheduling” by Benjamin Ransford, Shane Clark, Mastooreh Salajegheh, Kevin Fu. In *USENIX Workshop on Power Aware Computing and Systems (HotPower 2008)*, 6 pages, December 2008.

[W7] “Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security” by Tamara Denning, Kevin Fu, and Tadayoshi Kohno. In *USENIX Hot Topics in Security Workshop (HotSec)*, 7 pages, July 2008, (acceptance=32%).

[W8] “Cryptanalysis of Two Lightweight RFID Authentication Schemes” by Benessa Defend, Kevin Fu, and Ari Juels. In the *Proceedings of Fourth IEEE International Workshop on Pervasive Computing and Communication Security (PerSec) Workshop*, 5 pages, March 2007 (acceptance=29%).

[W9] “Secure Software Updates: Disappointments and New Challenges” by Anthony Bellissimo, John Burgess, and Kevin Fu. In *USENIX Hot Topics in Security Workshop (HotSec)*, 7 pages, July 2006 (acceptance=19.6%).

[W10] “Privacy for Public Transportation” by Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu. In *6th Workshop on Privacy Enhancing Technologies*

(PET), Lecture Notes in Computer Science, Vol. 4258, pp. 1–19, June 2006 (acceptance=26%).

**Book
chapter**

[B1] “Maximalist Cryptography and Computation on the WISP UHF RFID Tag” by Hee-Jin Chae, Mastrooreh Salajegheh, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu. Book chapter in *Wirelessly powered sensor networks and computational RFID*, Joshua R. Smith (ed.), 12 pages, to appear (earlier version in RFIDSec 2007).

**Invited
columns**

[Col1] “Inside Risks, Reducing Risks of Implantable Medical Devices: A Prescription to Improve Security and Privacy of Pervasive Health Care” by Kevin Fu. Inside Risks Column in *Communications of the ACM (CACM)* 52(6), June 2009.

[Col2] “Using SFS for a Secure Network File System” by Kevin Fu, Michael Kaminsky, and David Mazières. In *login: The USENIX Magazine*, December 2002.

[Col3] “Web Cookies: Not Just a Privacy Risk” by Emil Sit and Kevin Fu. Inside Risks Column in *Communications of the ACM (CACM)* 44(9):120, September 2001.

**Commissioned
paper**

[Com1] “Trustworthy Medical Device Software” by Kevin Fu. In *Public Health Effectiveness of the FDA 510(k) Clearance Process*, IOM (Institute of Medicine), National Academies Press, Washington, DC, 2011.

**Unrefereed
articles,
demos, and
posters**

[U1] “Software issues for the medical device approval process” by Kevin Fu. Statement to the Special Committee on Aging, United States Senate, Hearing on a delicate balance: FDA and the reform of the medical device approval process, Wednesday, April 13, 2011.

[U2] “Hybrid-powered RFID sensor networks” by Shane S. Clark, Jeremy Gummesson, Kevin Fu, Deepak Ganesan. Demo at ACM SenSys 2009.

[U3] “Privacy of home telemedicine: Encryption is not enough (poster)” by Mastrooreh Salajegheh, Andres Molina, Kevin Fu. Presented at *Design of Medical Devices Conference*, Minneapolis, MN, April 2009.

[U4] “Protecting Global Medical Telemetry Infrastructure” by Benessa Defend, Mastrooreh Salajegheh, Kevin Fu, Sozo Inoue. Institute of Information Infrastructure Protection (I3P), Technical Report, January 2008.

[U5] “Demonstration of an RFID-enabled espresso machine” by Hee-Jin Chae, Benessa Defend, and Kevin Fu. MIT RFID Academic Convocation, January 2006.

[U6] “In Memory of David Huffman.” In *ACM Crossroads Magazine* 6(3), Spring 2000.

[U7] “RTLinux: An Interview with Victor Yodaiken.” In *ACM Crossroads Magazine* 6(1), Fall 1999.

[U8] “Linux” (guest editor). In *ACM Crossroads Magazine* 6(1), Fall 1999.

[U9] “Group Sharing and Random Access in Cryptographic Storage File Systems.” MIT MEng Thesis, May 1999.

[U10] “Approximate Message Authentication Codes” by Richard Graveman and Kevin Fu. In *Army Research Labs, Advanced Telecommunications & Information Distribution Research Program*, February 1999.

[U11] “Networks and Distributed Systems” (guest editor). In *ACM Crossroads Magazine* 5(2), Winter 1998.

Research funding

[G1] Microsoft Research. \$7,500. PI: Kevin Fu. 4/2011–.

[G2] UMass Commercial Ventures & Intellectual Property (CVIP) Technology Development Fund Award: “SMASH Memory: Smarter Storage for Low Power Devices.” \$25K. PI: Kevin Fu. 3/2011–3/2012.

[G3] Armstrong Fund for Science at UMass Amherst: “Security and Privacy for Wirelessly Controlled Healthcare Technology.” \$20K. PI: Kevin Fu. 8/2010–7/2012.

[G4] HHS SHARP Security: “Strategic Healthcare IT Advanced Research Projects on Security (SHARPS).” \$15M (\$727K UMass). Lead UIUC PI: Carl Gunter. UMass CoPI: Kevin Fu. 4/2010–2/2014.

[G5] NSF Trustworthy Computing: “TC: Medium: Collaborative Research: Pay-as-you-Go: Security and Privacy for Integrated Transportation Payment Systems.” \$1,175K (\$844,997 UMass). PI: Wayne Burleson. CoPIs: John Collura, Kevin Fu, Anna Lysyanskaya, Christof Paar, Marguerite Zarrillo. NSF CNS Award #0964641. 6/2010–5/2013.

[G6] NSF Major Research Instrumentation: “MRI: Acquisition of an RFID Testbed Using Renewable Energy for Object Identification and Habitat Monitoring.” \$450,010. PI: Kevin Fu. CoPIs & Sr. Pers.: Charles Ross, Yanlei Diao, Deepak Ganesan, Wayne Burleson, Mark Corner, Prashant Shenoy. NSF CNS Award #0923313. 10/2009–9/2012.

[G7] NSF Trustworthy Computing: “CAREER: Computational RFID for Securing Zero-Power Pervasive Devices.” \$400K. PI: Kevin Fu. NSF CNS Award #0845874. 9/2009–8/2014.

Supplement: REU (\$16K) 5/2010–8/2014.

[G8] US Dept. of Transportation, MIT Subcontract: “Integrated Transportation Payment Systems: Principles, Concepts, and Applications” \$33,914. PI: John Collura, CoPIs: Wayne Burleson, Kevin Fu. 9/2009–8/2011.

[G9] National Security Agency/Dept. of Defense: “A Student Research Education Program in Information Command and Analysis” \$100,015. PI: Brian Levine. CoPIs: Mark Corner, Kevin Fu, David Jensen, Jerome Miklau. NSA H98230-09-1-0399. 9/2009–8/2010

[G10] Alfred P. Sloan Research Fellowship. \$50K. PI: Kevin Fu. 9/2009-8/2011.

[G11] NSF Cyber Trust: “CT-ISG: Improving Security and Privacy in Pervasive Healthcare.” \$449,685. PI: Kevin Fu. NSF CNS Award #0831244. 9/2008–8/2011.

Supplement: REU (\$16K) 6/2009–8/2011.

[G12] UMass President's Science & Technology (S&T) Fund "Integrated Payment Systems: Consortium on Security and Privacy." \$125K. PI: Wayne Burleson. Co-PIs: John Collura, Kevin Fu, Marguerite Zarrillo. 8/2008-7/2010.

[G13] Institute for Information Infrastructure Protection (I3P) at Dartmouth College: "I3P Scholar Program. Research on Securing Medical Cyberinfrastructure." \$90K. PI: Kevin Fu. Scholar: Shane Clark. 8/2008-8/2009.

[G14] UMass Commercial Ventures & Intellectual Property (CVIP) Technology Development Fund Award: "Zero-Power Telemetry for Implantable Medical Devices." \$30K. PI: Kevin Fu. 6/2008-5/2009.

[G15] Institute for Information Infrastructure Protection (I3P) at Dartmouth College: "Protecting Global Medical Telemetry Infrastructure." \$25K. PI: Kevin Fu. 11/2007-12/2007.

[G16] NSF Cyber Trust: "Collaborative Research CT-ISG: New Directions and Applications of Proxy Re-cryptography." \$276,142 (\$62,980 UMass, \$213,163 JHU). Lead JHU PI: Susan Hohenberger. JHU CoPI: Giuseppe Ateniese. UMass CoPI: Kevin Fu. NSF CNS Award #0716386. 9/2007-8/2010.
Supplement: REU (\$16K) 6/2009-8/2010.

[G17] Gifts from RSA Labs (Security Division of EMC Corporation). \$10K, 2006-2007; \$40K, 3/2008-. PI: Kevin Fu.

[G18] Intel Research Seattle. RFID equipment donation valued at \$7,600, 2007. PI: Kevin Fu

[G19] ThingMagic. RFID equipment donation valued at \$5K, 2007. PI: Kevin Fu.

[G20] NSF Cyber Trust: "Collaborative Research CT-T: Security for Smart Tags." \$1.1 million (\$750K UMass, \$350K JHU). Lead PI: Kevin Fu. CoPIs & Sr. Pers.: Wayne Burleson, Adam Stubblefield (JHU), Ari Juels (RSA Labs). NSF CNS Award #0627529. 9/2006-8/2010.

Supplements: Travel for collaboration in Japan (\$40K) 9/2007-8/2009; REU (\$15K) 6/2007-8/2008; REU (\$6K) 6/2008-8/2009; Travel for collaboration in France and Switzerland (\$15K) 6/2009-8/2010; JHU Subcontract (\$50K) 8/2009-7/2010.

**Invited
talks and
panels since
joining UMass**

[T1] Keynote speaker, "The Cutting Edge of Medical Device Security and Privacy," 14th International Symposium on Recent Advances in Intrusion Detection (RAID 2011), Menlo Park, CA, September 2011.

[T2] Invited speaker, "Trustworthy Medical Device Software."
Duke University, Durham, NC, November 2011
Johns Hopkins University Distinguished Lecture, Baltimore, MD, October 2011
Department of Homeland Security InfoSec Technology Transition Council, 2011
UC Irvine, Irvine, CA, May 2011
Williams College, Williamstown, MA, April 2011

Univ. Pennsylvania PRECISE, Philadelphia, PA, April 2011
UCSB, Distinguished Undergraduate Lecture Series, Santa Barbara, CA, April 2011
EPFL Workshop on Security/Privacy of Implantable IMDs (SPIMD), Lausanne, Switzerland, April 2011
Ruhr-Universitt Bochum, Lehrstuhl Embedded Security, Bochum, Germany, March 2011
Rice University, Computer Science Colloquium, Houston, TX, October 2010
5th Workshop on Embedded Systems Security (WESS10), Scottsdale, AZ, October 2010

[T3] Distinguished Lecture, Johns Hopkins University, Computer Science, October 2011.

[T4] Invited speaker, “Your Abstractions are Worth^H^H^H^HPowerless! Non-Volatile Storage and Computation on Embedded Devices* (*Batteries Not Included).”
New York University, NY, NY, December 2011
Microsoft Research, Redmond, WA, July 2011
University of Washington, Seattle, WA, July 2011
EMC, Cambridge, MA, June 2011
Rambus, Sunnyvale, CA, May 2011

[T5] Invited speaker, “Medical Device Security and Privacy Concerns,” National Institute of Standards and Technology (NIST) Information Security and Privacy Advisory Board (ISPAB), Washington, DC, July 2011.

[T6] Invited panelist, “Hackers and Attackers: How Safe is Your Embedded Design,” Design Automation Conference (DAC), Embedded Systems and Software, San Diego, CA, June 2011.

[T7] Invited panelist, “Can I Hack Your Brain?” IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST), San Diego, CA, June 2011.

[T8] Invited panelist, CES/Amphion Forum, Las Vegas, NV, January 2011.

[T9] Invited participant, National Academy of Engineering, U.S. Frontiers of Engineering Symposium, Armonk, NY, September 2010.
<http://www.naefrontiers.org/>

[T10] Distinguished speaker, 2nd ACM S³ Workshop on Wireless of the Students, by the Students, for the Students, Chicago, September 2010.

[T11] Invited speaker, “Trustworthy Medical Device Software,” Institute of Medicine at the National Academies of Science panel on Public Health Effectiveness of the FDA 510(k) Clearance Process, Washington, DC, July 2010.
<http://www.iom.edu/Activities/PublicHealth/510KProcess/2010-JUL-28.aspx>

[T12] Invited panelist, “Reliability—How to Define Quality of Service,” Joint FCC–FDA Public Meeting: Enabling the Convergence of Communications and Medical Systems, Washington, DC, July 2010.
<http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm215046.htm>

[T13] Invited speaker, “Trustworthy Computing,” Presidents Innovation and Technology Advisory Committee (PITAC), Washington, DC, June 2010.

[T14] Invited speaker. “Implantable Medical Devices: Security and Privacy for Pervasive, Wireless Healthcare,” Dartmouth College Computer Science Colloquium, Hanover, NH, April 2010.

[T15] Invited speaker. “Implantable Medical Devices: Security and Privacy for Pervasive, Wireless Healthcare,” Samsung Research, Dallas, Texas, January 2010.

[T16] Invited speaker. “Cooking Scientific Discovery,” Annual Make-a-Difference Conference, Hong Kong, January 2010.

[T17] Invited speaker. “MIT Emerging Technologies Symposium (EmTech 2009),” Cambridge, September 2009.

[T18] Invited speaker. “MIT Bankcard Payment Workshop,” Cambridge, MA, September 2009.

[T19] Invited speaker. “Workshop on Confidential Data Collection for Innovation Analysis in Organizations,” Redmond, WA, September 2009.

[T20] Invited speaker. “Implantable Medical Devices: Security and Privacy for Pervasive Wireless Healthcare,” CMU CyLab Seminar, Pittsburgh, PA, March 2009.

[T21] Invited speaker. “Security and Privacy for Wireless Implantable Devices: Pacing, Defibrillators, and More,” CMOS Workshop, Banff, Canada, February 2009.

[T22] Invited speaker. “Energy-Aware Circuits for RFID,” CMOS Workshop, Banff, Canada, February 2009.

[T23] Invited speaker. “Implantable Medical Devices: Security and Privacy for Pervasive, Wireless Healthcare,” University of Massachusetts Amherst, Isenberg School of Management, The Institute for Operations Research and the Management Sciences (INFORMS) Seminar Series, December 2008.

[T24] Invited speaker. “Security Vulnerabilities in Wireless Implantable Medical Devices,” Microsoft Research Redmond, September 2008.

[T25] Invited speaker. “Implantable Medical Devices: Security and Privacy for Pervasive, Wireless Healthcare,” Johns Hopkins University Security Seminar Series, September 2008.

[T26] Invited speaker. “Security Vulnerabilities in Wireless Implantable Medical Devices,” UMass Amherst ECE Security Seminar, September 2008.

[T27] Invited speaker. “Security Vulnerabilities in Wireless Implantable Medical Devices,” Texas Instruments, September 2008.

[T28] Invited co-speaker. “New Classes of Security and Privacy Vulnerabilities for Implantable Wireless Medical Devices,” Black Hat USA Briefings 2008, Las Vegas, August 2008.

[T29] Invited speaker. “Pay on the Go: Consumers & Contactless Payment” Federal Trade Commission Town Hall Meeting, Seattle, July 2008.

[T30] Invited panelist. “Is it Legal?” Panel on wireless privacy and security at the ACM/USENIX MobiSys Conference, Denver, June 2008.

[T31] Invited panelist. “RFID Security & Privacy: What’s in Your Pocket?” 8th Payments Conference: Payments Fraud, Perception versus Reality hosted by the Federal Reserve Bank of Chicago, June 2008.

[T32] Invited Speaker. “Maximalist Cryptography and Computation on the WISP UHF RFID Tag,” Intel Research Seattle, January 2008.

[T33] Invited Speaker. “I Can See You: RFID — The Next Generation Identity Theft Threat,” 17th Annual International Fraud Investigators Conference hosted by the Toronto Police Service-Fraud Squad, December 2007.

[T34] Invited Speaker. “Security & Privacy for Pervasive Computation: RFID and Implantable Medical Devices,” EMC Corporation Innovation Conference, Franklin, MA, October 2007.

[T35] Invited Speaker. “RFID Security and Privacy: Fundamental Lessons and Principles,” 19th Workshop on Info. Sec. and Cryptography, Cheonan, Korea, September 2007; National Security Research Institute, Daejeon, Korea, September 2007; Korea University, Division of Computer & Comm. Eng., Seoul, Korea, September 2007.

[T36] Invited Panelist. “RFID Privacy,” MITRE Privacy Technical Exchange, Bethesda, MD, June 2007.

[T37] Invited Speaker. “Data Security Risks: RFID Lab Research,” Boston Federal Reserve, Emerging Payments Research Group, May 2007.

[T38] Invited Panelist. “Ubiquitous Computing in the Retail Store of the Future,” 17th Annual Computers, Freedom and Privacy Conference, May 2007.

[T39] Invited Panelist and Moderator. “Wireless ID Issues: Privacy, Efficiency and Security,” Dartmouth College Centers Forum on Freedom and Technology, April 2007.

[T40] Invited Speaker. “Vulnerabilities in First-Generation RFID-Enabled Credit Cards,” UC Berkeley TRUST seminar, March 2007; Katholieke Universiteit (KU) Leuven Seminar, Belgium, March 2007.

[T41] Invited Panelist. “RFID: How Can Privacy and Security Be Built into the Technology,” 8th Annual TACD Meeting with EC and US government officials, Brussels, Belgium, March 2007 (<http://www.tacd.org/events/meeting8/>).

[T42] Panel Moderator. “RFID Security & Privacy Panel,”
Financial Cryptography Conference, Tobago/Trinidad, February 2007.

[T43] Invited Speaker. “Computer System Security and Medical Devices,”
Food and Drug Administration (FDA), Office of Science and Engineering Laboratories,
Center for Devices and Radiological Health, October 2006.

[T44] Invited Speaker. “Building RFID Applications with Security and Privacy,”
Workshop on RFID Security, Graz, Austria, July 2006.

[T45] Invited Panelist. “When Public Databases Cause Security Vulnerabilities,”
American Association for the Advancement of Science (AAAS), St. Louis, MO, February,
2006.

**Professional
service:
leadership**

NIST Information Security and Privacy Advisory Board Washington, DC
The Board provides advice on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST. The Board reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Congressional committees.
Board Member: *October 2011–*.

ACM SIGCOMM Workshop on Medical Communication Systems Helsinki
Program Chair of MedCOMM: *August 2012*.

USENIX Health Security and Privacy Workshop (HealthSec)
Co-Founder. Steering Group Member: *2010–*. Co-Chair: *August 2010*. Member: *August 2011*

RFID Security Conference/Workshop (RFIDSec) Europe
General Chair: *June 2011*. Steering Group Member: *September 2007–*.

**Workshop on Wirelessly Powered Sensor Networks
and Computational RFID (WISP Summit)** Berkeley, CA
Co-Chair: *November 2009*.

Privacy Enhancing Technologies (PET) Award Selection Committee
Selection committee, PET Outstanding Research Award. *June 2010*.

MIT TR35 Award Selection Committee
Selection committee, MIT Technology Review’s TR35 awards. *April 2010*.

Institute for Information Infrastructure Protection (I3P) Hanover, NH
UMass Amherst representative: *July 2007–*.

**Professional
service:
program
committees**

Dependable Computing and Communications Symposium (DCCS) Boston, MA
Member: *June 2012*

IEEE Symposium on Security & Privacy Oakland, CA
Member: *May 2011, May 2009, May 2008, May 2006.*

USENIX Security Symposium
Member: *August 2012, August 2007, August 2003, August 2002.*

World Wide Web Conference: Security, Privacy, Reliability and Ethics Track
Member: *May 2007, May 2006, May 2003.*

**ACM Workshop on Security and Privacy
in Medical and Home-Care Systems (SPIMACS)** Chicago, IL
Member: *November 2009.*

**ACM Conference on
Embedded Networked Sensor Systems (SenSys)** Berkeley, CA
Member: *November 2009.*

**ACM/USENIX International Conference on
Mobile Systems, Applications, and Services (MobiSys)** Kraków, Poland
Member: *June 2009.*

**International Conference on
Financial Cryptography and Data Security** Cozumel, Mexico
Member: *January 2008.*

**International Conference on
Applied Cryptography and Network Security (ACNS)** Zhuhai, China
Member: *June 2007.*

Network & Distributed System Security Symposium San Diego, CA
Member: *February 2006, February 2004.*

IEEE International Security in Storage Workshop (SISW) San Francisco, CA
Member: *December 2005.*

The Storage Security and Survivability (StorageSS) Workshop Fairfax, VA
Member: *November 2005.*

National Science Foundation Arlington, VA
Panelist and reviewer: *2005–.*

Patents issued “Method and System for Relating Cryptographic Keys” by Kevin Fu, Mahesh Kallahalla, Ram Swaminathan. US patent #7,313,238. Hewlett-Packard Labs. Filed 2003. Issued 2007.

“Windowed Backward Key Rotation” by Kevin Fu, Mahesh Kallahalla, Ram Swaminathan. US patent #7,697,690. Hewlett-Packard Labs. Filed 2003. Issued 2010.

Patents pending “Methods and Systems for Zero-Power Time Keeping” by Kevin Fu, Jacob Sorber, Mas-tooreh Salajegheh. December 2011.

“Methods and Systems for Low-Power Storage for Flash Memory” by Kevin Fu, Erik Learned-Miller, Mastroeh Salajegheh. December 2010.

“Systems and Methods for Zero-Power Security” by Kevin Fu. October 2008.

“Unidirectional Proxy Re-encryption” by Susan R. Hohenberger, Kevin Fu, Giuseppe Ateniese, Matthew Green. Publication US 2008/0059787 filed February 2006.

Degrees conferred

Masters of Science (advisor role)

Hee-Jin Chae (2007), Benessa Defend (2008), Shane Clark (2011), Thomas S. Heydt-Benjamin (2007), Robert Lychev (2008), Benjamin Ransford (2010).

Current students

PhD track (advisor role)

Shane Clark (NSF Fellow), Andres Molina-Markham, Amir Rahmati, Benjamin Ransford (NSF Fellow), Mastroeh Salajegheh.

Masters track (advisor role)

Hong Zhang, Shane Guineau.

Thesis committees

Thesis committees outside CS department (member role)

Daniel Holcomb (ECE, masters 2007), Lang Lin (ECE, masters 2009), Ashwin Lakshminarasimhan (ECE, masters in progress), Penny Ridgill (Math, PhD 2009), Weifeng Xu (ECE, PhD 2007), Serge Zhilyaev (ECE, masters 2010).

Thesis committees outside UMass Amherst (member role)

Shyamnath Gollakota (MIT EECS, PhD in progress).

Undergraduate research

REUs
John Brattin (CS, 2009), Shane Clark (CS, 2006-07), David Eiselen (ECE, 2007), Teresa Fiore (REU, 2011), Shane Guineau (CS, 2011), Andrew Hall (REU, 2011), Nicole Kaufman (REU, 2011), Olga Korobova (REU, 2011), Jean Fredo Louis (REU, 2008), Erin McBride (REU, 2011), William Morgan (CS, 2007), Rene Santiago (ECE, 2007), Deepti Sreepathi (microbiology, 2009), Quinn Stewart (REU, 2009-), John Tuttle (CS, 2008), Zak Wirima (REU, 2008), Vladislav Yazhbin (CS, 2009-10), Mankin Yuen (CS, 2008).

Teaching

CMP SCI 201: Architecture & Assembly Language (4 credits)

Spring 2009, 2010. Instructor. ~30 students. Introduction to the architecture and machine-level operations of modern computers at the logic, component, and system levels.

CMP SCI 466 Applied Cryptography (3 credits, previously CMP SCI 591D)

Fall 2010, Spring 2008, Spring 2007, Spring 2006. Instructor. ~20 students. Teaches upper-level undergraduates the foundations of applied cryptography and the humility of building practical systems that rely on cryptography.

CMP SCI 615/691CC: Advanced Information Assurance (3 credits)

Fall 2007, instructor; Fall 2006, co-instructor. Teaches graduate students the foundational material to enter the research community of information assurance.

MIT's Network and Computer Security (6.857)

Head TA and guest lecturer (Fall 2001, Fall 2002). ~80 undergraduate/graduate students.

MIT's Computer System Engineering (6.033)

Head TA (Spring 1999), TA (Spring 1998). ~300 students.

MIT's Computer System Engineering Lab (6.906)

Lab TA (Spring 1998, Spring 1999).

CMP SCI 191A: First-Year TAP Seminar (1 credit)

Fall 2006, co-organizer. This seminar introduces first-year undergraduates to major topics in Computer Science. Each week there is a new guest lecturer.

CMP SCI 291E: RFID Electronic Identification Lab (1 credit)

Fall 2007. Instructor. My lab taught sophomores about hands-on problem solving in the context of RFID.

CMP SCI 691I: Hot Topics in Information Security (1 credit)

Fall 2007, instructor; Fall 2005, co-instructor. This seminar covers cutting-edge papers to identify novel research problems in security.

RFID Security and Privacy Tutorial (1 day)

USENIX Security Tutorial by Kevin Fu, Ari Juels, and Adam Stubblefield. Vancouver, Canada, August 2006.

RFID Security Summer School (1 lecture)

“Special topics in RFID security,” Technical University of Graz, Austria, July 2006.

MIT's Introduction to the Theory of Computation (6.840)

Grader (Fall 1998).

Departmental service

Admissions Committee, 2006–2007, 2009–2010, 2010–2011;
Awards Committee, 2009–2010;
Computing Committee, 2005–2006, 2006–2007;
Distinguished Lecture Series (DLS)/Special Events Chair, 2008–2009;
ECE Senior Faculty Search Committee, 2008–2009;
Graduate Program Committee, 2007–2008, 2008–2009;
Personnel Committee, 2007–2008;
Recruiting Committee, 2005–2006.

Other service

Ad hoc reviewer

ACM Transactions on Information and System Security (TISSEC); IEEE/ACM Transactions on Networking (TON); ACM Transactions on Sensor Networks (TOSN); ACM Transactions on Computer Systems (TOCS); NordSec; IEEE Security & Privacy Magazine; IEEE Internet Computing; International Conference on Distributed Computing Systems (ICDCS); International Workshop on Information Security Applications (WISA); USENIX Annual Technical Conference; Symposium on Operating Systems Principles (SOSP); USENIX Conference on File and Storage Technologies (FAST); International

Workshop on Peer-to-Peer Systems (IPTPS); Workshop on Hot Topics in Operating Systems (HotOS); Symposium on Operating Systems Design and Implementation (OSDI).

Graduate Resident Tutor — MIT Residential Life Burton-Conner

As a live-in “life” tutor for 30 undergraduates, I facilitated conflict resolution, off-campus retreats, medical emergencies, and culinary productions. 2000–2003.

Academic Advising — MIT Department of EECS Cambridge, MA

Associate academic advisor to help undergraduates develop their four-year academic plans. Co-advised with Alex d’Arbeloff, MIT Chairman of the Corporation. 1999–2003.

Association of Computing Machinery New York, NY

General editor and contributor to the *ACM Crossroads Magazine*. 1998–2000
(<http://www.acm.org/crossroads/>).

French Culinary Institute New York, NY

Received certificate of achievement in artisanal bread making while producing the bread for the student-run L’Ecole restaurant. June 2004.

Selected media coverage of research “Medical device software criticized as under-regulated” by Christine Mai-Duc. In *Los Angeles Times*, September 1, 2011.

“Headphones Can Disrupt Implanted Heart Devices” by Joseph Shapiro. In *National Public Radio, All Things Considered*, October 22, 2009.

“A Heart Device Is Found Vulnerable to Hacker Attacks” by Barnaby J. Feder. In *The New York Times*, Business Section, Mar 12, 2008.

“Heart-Device Hacking Risks Seen” by Keith J. Winstein. In *The Wall Street Journal*, March 12, 2008.

“Questions on Credit Card Safety” by John Schwartz. In *The New York Times*, Business Section, Page B1, October 23, 2006.